(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 March 2005 (24.03.2005)

PCT

(10) International Publication Number
WO 2005/026872 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/IL2004/000849

(22) International Filing Date:
14 September 2004 (14.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/502,940 16 September 2003 (16.09.2003) US

(71) Applicant *(for all designated States except US)*: TERASSIC-5 INFOSEC LTD [IL/IL]; 25 Yam Hamelah st., 55900 Ganey -Tikva (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: RAVIV, Raz [IL/IL]; 25 Yam Hamelah st., 55900 Ganey -Tikva (IL).

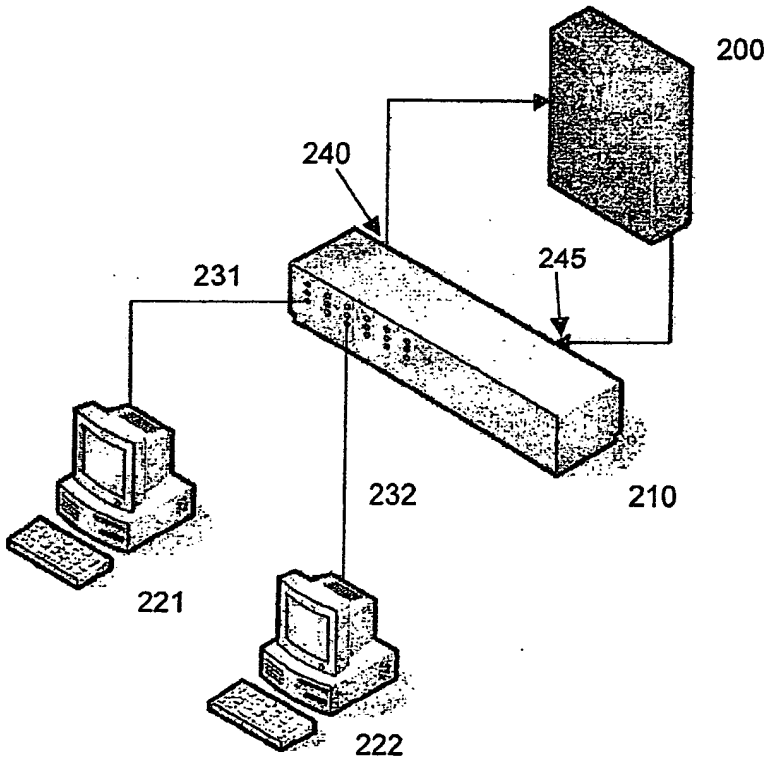
(74) Agent: APPELFELD ZER LAW OFFICE; 29 Lilinblum, 65133 Tel-aviv (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: INTERNAL LAN PERIMETER SECURITY APPLIANCE COMPOSED OF A PCI CARD AND COMPLEMENTARY SOFTWARE



(57) Abstract: A system for providing LAN security which operates on communication Layers 2 to 7 is disclosed. The system is comprised of a PCI card which performs the monitoring of the communication on the LAN, statistical analysis of data traffic and implements fuzzy logic and protocol flow inspection for identifying any abnormal and suspicious communication activity. It is composed of a hardware network interface, whose presence on the network is invisible to the network users, and of an additional interface issuing session interception signals. Using discriminate functions classing, the system can learn to recognize and differentiate anomalous traffic within standard network signals. The system is equipped for rapid recognition of known and unknown malicious activities within routine network traffic. Coupled with known protocol flow comparison, the system detects masquerading, eavesdropping, scanning, denial-of-service attacks and "hacking" attempts. The system also performs network communication flow optimization and hardware performance enhancement.

WO 2005/026872 A2

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Internal LAN Perimeter Security Appliance Composed of a PCI Card and complementary software

BACKGROUND

The invention relates to communication networks, and more particularly to a system method and apparatus for providing secure internetworking of LAN using intra-network hardware implementations.

Security management systems prevalent in prior art mainly address security at high networking communication layers, primarily on the application or session layer. Although network intrusions occur frequently, most intrusion detection methods disclosed in the prior art are incapable of recognizing intrusions through the lower layers of network communication transmission protocols and hardware connections.

Following is a description of the most prevalent securing methods. Traditionally, pure Intrusion Detection Systems (IDS) serve basically as traditional sniffers, hooked onto a database of known intrusion attacks. Basically IDS compares each packet, which is sniffed off the live network traffic, against the known attack signatures database. In case a match is found, an alert is recorded in a log for later analysis, or propagated to the system administrator via the network. Most current day IDS's contain the ability to send a session-kill signal to a designated border-gateway, such as a router or firewall. In this manner, an entry is added to the gateway's Access Control List, in order to prevent further inbound access from the malicious activity within a specific network session.

The most widely used method of terminating a network session at the gateway is carried out by sending both conversing parties an RST packet. This RST packet, as defined within the Transmit Control Protocol (TCP) notifies the system currently in session that an error has occurred in the communication flow. Thus, each side of the session is expected to cease communication and flush whatever data has been accumulated within its memory buffer.

In order to invocate a session reset, a third party device must satisfy the following requirements: it must serve as gateway in between the two conversing parties; it must be trusted by both parties to manage the routing and data transference between them; and it must know the Initial Sequence Number (ISN), and calculate the offset of the packet numbering from the beginning of the session. Having satisfied the above requirements, the gateway may masquerade as party A, whilst sending an RST packet to party B, and vice versa. This enables it to disconnect the TCP session.

However, a User Datagram Protocol (UDP) session, by definition, is not connection based, and therefore will not be affected by a session reset attempt as described above. In order to handle both UDP and TCP sessions, and maintain the ability to drop any session at request, firewalls sometimes work in what is known as inline mode. In this mode, two different network interfaces are utilized to connect the two sides of the network border. During regular communication flow, packets are routed from one network interface card (NIC) to another whilst the firewall device serves as a regular network bridge. In the event that a session needs to be terminated, all packets belonging to the specific session are dropped at the firewall instead of passing from the external NIC to the internal one. The only requirement for this work mode is that the firewall resides physically in between the two conversing parties, segmenting the two sides into two different networks.

Currently there are several networking equipment manufacturers which enable the switch administrator to define a pool of allowed MAC addresses per network port. This allows the administrator to enforce MAC security at the backbone level, preventing unknown NICs from connecting and establishing communication at layer-1. This definition needs to be configured manually per switch, which might be troublesome in certain switches, when working with roaming computers, such as laptops.

The 802.1X standard protocol derives its design both from the dial-up and the wireless networking world as a hybrid protocol. Based on the underlying Extensible Authentication Protocol (EAP), the 802.1X protocol enables user-authentication to be carried-out, prior to enabling access to the network backbone. As a user attaches to a network switch with the intent of using the network port for communication with the rest of the network, he/she must supply a username/password or a security certificate. For this aim, an 802.1X server, such as RADIUS, must be installed and configured in order to manage a user repository.

Since most current intrusion detection systems focus on traffic on network's layer-3 and above, a spoofed IP address can easily pass for a legitimate node on the internal network. The nature of the Address Resolution Protocol (ARP) and Reversed Address Resolution Protocol (RARP) may be exploited is such manner. Since the ARP has no authentication method implemented according to RFC requirements, any station with physical access to the network backbone may forge its identity.

Thus, intruders wishing to masquerade as legitimate network nodes need only connect to a physical port connection in one of the network switches, in order to publish their unique MAC address bound to a legitimate, working IP address of a different computer. As long as the ARP broadcasts keep racing frequencies with the legitimate stations, the network will respond to both seamlessly, as though they were the same station. In this method, the intruder may play the role of a Man-In-The-Middle (MITM), by

reading the misdirected traffic, subsequently retransmitting it to the legitimate destination, thus maintaining transparency. Some software systems have the ability to transmit alerts upon the connection of a previously-unknown Mac address to the network. However, these systems are not able to intercept such attacks, nor are they able to locate the location at which the intrusion has occurred.

It is therefore the object of the present invention to provide a network intrusion detection and prevention system (NIDP) based on identification and interception of unauthorized user communication thereof.

SUMMARY

A system for network intrusion detection and prevention which is implemented on PCI chip card is disclosed. The system includes management of network security and access control, while the card activity is transparent to network communication. The system is comprised of a monitoring module for tracking and recording data traffic on all communication layers (layer 2 to layer 7) wherein the data includes port switches, MAC addresses and IP Addresses; a learning module for recognizing anomalous traffic data within standard network signals; an analyzing module for identifying suspicious activity on the local network wherein the analysis is based on fuzzy logic rules which are applied on monitored data and recognized patterns of anomalous traffic data are used; and security module for alerting or activating prevention activities upon detection of suspicious activity.

The system also includes a comparison module for checking new transmission data against authorization table of known correlation of IP addresses, port switches and MAC addresses. It prevents eavesdropping for identifying Address Resolution Protocol (ARP) spoofing based on statistical analysis and layer-2 network state monitoring. The eavesdropping prevention module includes a Dynamic Host Configuration Protocol

(DHCP) analyzer. The prevention activities include interception of session at application level, denying access to a specific switch block for controllable time interval or completely blocking access through a given switch port.

A user interface module provides graphic representations of network traffic wherein abnormal patterns of suspicious communication data are identified. An assessment module receives data from vulnerability assessment tool and improves the monitoring and analysis of network traffic data.

A load balancing module is also included, which operates based on analyzed traffic data as well as a defragmentation module for checking the data packets at their original form. A filtering model checks packets headers and filters data packets before reaching any software modules. Filtering is based on source/destination MAC and IP addresses, network ports, switch ports or protocol type data which is stored in the card memory. The system also performs traffic normalization based on bargain-point equilibrium formulas, for achieving a state of relatively fair allocation of bandwidth among network nodes. Bandwidth allocation is based on statistical history data of typical usage of bandwidth per workstation and online behavior of the consumed bandwidth per specific network nodes.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of prior art;

Figure 2 is a schematic illustration of the traffic flow according to the preferred embodiment of the present system;

Figure 3 is a block diagram illustrating the high-level design view of hardware modules according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention includes a monitoring system for tracking and recording data traffic on all communication layers (layer-2 through layer-7) and an analysis module based on fuzzy logic and protocol flow inspection, for identifying any suspicious activity on the local network. It is composed of a hardware network interface, whose presence on the network is invisible to the network users, and of an additional interface issuing session interception signals. Using discriminate functions classing, the system can learn to recognize and differentiate anomalous traffic within standard network signals. Implemented at chip level, fuzzy logic Digital Signal Processing (DSP) technology enables rapid recognition of known and unknown malicious activities within routine network traffic. Coupled with known protocol flow comparison, the system detects masquerading, eavesdropping, scanning, denial-of-service (DoS) attacks and "hacking" attempts.

The monitoring system includes the examination of new communication transmissions, correlating IP addresses (Utilizing DHCP Listening), MAC Addresses and port switch with updated table of authorized connections. Unknown or new combinations are marked as possible intrusions. A foreign (out-of-office) network card (NIC) by default cannot connect to the local network unless permission is granted by the manager. Any appearance of a new or a duplicate pair of IP-MAC addresses automatically alerts the system.

Address Resolution Protocol (ARP) spoofing is the most widely used method for local network penetration and invisible data communication eavesdropping. This type of intrusion cannot be prevented by most access control systems, especially when operated in combination with MAC spoofing. By keeping both system level and hardware level under surveillance, the system is able to maintain the network's integrity and to protect it from intrusion by local and foreign ARP spoofing.

The system's intrusion detection module incorporates traditional IDS methods using packet signature matching in real-time, statistical anomaly detection in network traffic flow, as well as proprietary technology for detection of network eavesdropping attempts. The following technologies enable precise correlation of events detection, therefore ensuring mitigation of false positives and false negatives. A packet signature comparison is performed at wire-level implemented in ASIC technology within the PCI adapter. Network traffic passes from Ethernet adapter, through PCI accelerator into the communication bus of the system's appliance. Each TCP/IP packet traveling through the PCI adapter is compared against a database of known intrusion signatures, saved within the PCI adapter's on-board flash memory.

DHCP and ARP traffic is monitored at Layer-2 and saved as record tables. It is then compared against pre-configured defaults. In case a spoofed DHCP server, or MAC-IP pair is detected, the system alerts and acts against the offensive node. This mode of operation enables detection and counter-action against data sniffing and/or injection on network backbones, including hubs, switches and routers.

The system's fuzzy logic module bases its concept of work upon statistical behavior learning. At its initialization, the module examines patterns of traffic by passively monitoring the network backbone. After a period of a few days, the sampled patterns are grouped into discriminate clusters of vectors. Each group of vectors characterizes a range of traffic signals which share common frequencies and source/destination as well as other attributes. During the learning process, the clusters may expand and contract according to the convergence and divergence of their essential signals. Once the learning period has been satisfied, any traffic that seems too foreign to be classified within the known clusters triggers an alert. Based on prior academic researches, this method has proven to be effective in detection of network scans, Trojan horses, Denial-of-Service attacks and more.

Figure 1 is a schematic illustration of prior art and Figure 2 is a schematic diagram of traffic flows according to the preferred embodiment of the present invention. In contrast to the prevalent standards, as illustrated in Figure 1, in which firewall products 130 focus on filtering network traffic traveling between the outbound 110 and inbound 100 connections of a network while the malicious factors 140 may reside inside the network, the system 200 performs traffic filtering at the monitoring all network sessions 131, 132 flowing through the network backbone 110 between every two station 121, 122 on the network. A graphic user interface allows the administrator to define access policies for network stations and servers, identifying each node by its unique MAC address. At its normal operation, the system 200 monitors traffic through a NIC interface residing on a hub or a mirroring port 240 of the backbone switch 210. The system is also connected to an active standard full duplex port through which it can send commands. In the event of identifying an access violation, the network node which tries to establish the illegitimate session is automatically routed through the system 200 in order to filter the illegitimate activity, while still allowing the legitimate traffic originating from the same node to pass through. The filtering process is carried out in the following order. First the system 200 detects illegitimate traffic by its MAC and IP address, its port, or by intrusion signatures via an interface residing mirroring port. Then the system 200 identifies the conversing parties 221, 222, saves their MAC-IP pairings in its memory and begins ARP-Poisoning the two parties by feeding their ARP tables with spoofed MAC-IP pairs. These spoofed pairs lead whatever IP that may be looked up to the MAC address of system 200. Whenever one side of the communication 221 tries to establish a session with the other 222, it looks up the ARP table at the backbone 210, and finds the requested IP associated with the MAC of the system 200. From now on all traffic 231, 232 from both sides is routed to the system 200. The legitimate sessions are routed seamlessly via the system 200, while the illegal sessions' packets are dropped at

entrance. In this fashion, only traffic that has been deemed legal may reach its target. Once the illegal communication attempts ceases, the system 200 performs again the ARP process for both poisoned sides by sending ARP packets containing the real MAC-IP addresses. Thus the traffic 231, 232 continues without having to pass through the system continuously.

In cases where immediate and severe action must be taken against an intruder, the system may be configured (according to policy) to block or suspend switch ports which are detected as communicating illegal traffic. This is accomplished by continuously monitoring switch ports, in order to detect foreign MAC address connections, virus outbreaks and illegal network activities. Once such port has been identified, the system communicates using Telnet, Secure Shell (SSH) or Simple Network Management Protocol (SNMP) to issue block or suspend port commands to the backbone switch.

Another mode of operation which is supported by the system is timely information extraction from enterprise switches. The system may use SNMP commands once in a few minutes, in order to investigate whether new MACs have appeared on the sampled switch. In this case there is no need for sniffing; the system may reach remote switches, thus serve as a central Security Operations Center product.

Integrating an NIDP appliance and the network backbone enables the system to provide total layer-2 protection from physical intrusion attempts through "hot" network sockets left unmonitored within the office.

The system offers protection from internal and external DoS attacks by detecting internal load buildups on specific communication terminals. It identifies the signature pattern of the attacks and records it to prevent similar attacks in future.

The proposed system also operates as a hardware performance enhancer. A central network system such as a firewall, a router, a backbone switch, an information processing system (IPS) and the like demonstrate significant improvements in

performance, when electronic acceleration is integrated into its core. As regular PC-based operating systems are limited by resource requirements such as CPU cycles, RAM memory, HD swap space, task-oriented coprocessors are usually developed in the aims of offloading routine tasks from the operating system's resources. Specifically, the system is designed as an Application Specific Integrated Circuit (ASIC) processor implemented within a standard PCI-bus adapter.

As traffic flows through the system, several operations are carried out within the coprocessor. Whenever network packets exceed the maximum length possible for handling by a network router, the latter may device one packet into multiple sub-packets which are called fragments. Each fragment is labeled with a sequence number by its respective place in the original packet. Since Intrusion Detection systems need to examine the original packet as it appeared prior to the fragmentation process, these fragments need to be reassembled before entering the signature-database checking module. The system therefore automatically performs packet defragmentation.

The system also performs packet filtering. Commonly, within gateway firewalls, an Access Control List (ACL) is produced by the administrative user. Once the ACL has been established, these rules are interpreted into blocking criteria according to source/destination MAC and IP addresses, network ports, switch ports and protocol type. Consequently, network traffic is immediately filtered at entrance to the coprocessor, prior to reaching the software components. This is accomplished by storing an image of the ACL within the PCI card's volatile memory every time the system is brought online. Thus, for each frame traveling through the system's network interface, the above mentioned headers are inspected before allowing the packet to continue into the other modules. Header inspection also maintains qualification of each packet to satisfy normal RFC formats (countering XMAS, NULL, FIN and other network scans).

An additional feature of the system is that it provides a statistical traffic sampling tool. As mentioned in regards to the fuzzy logic module, network traffic is continuously sampled and analyzed for detection of anomalies over the time axis. As this is a resource-consuming rigorous task, the PCI adapter carries out the required measurements in parallel to the regular packet-header dissection. This allows seamless work of intrusion-detection, packet filtering and statistical-analysis modules simultaneously. Timely measurements and relative variances are propagated at arbitrary points in time onto the overlying operating system for long-term storage for training and learning about past incidents.

Finally the system may provide traffic normalization capabilities. Based on bargain-point equilibrium formulas, the system achieves a state of relatively-fair allocation of bandwidth among network nodes. Unlike traditional Quality of Service systems, the system is not configured with static parameters of bandwidth-quotas. Rather, it utilizes its statistical learning abilities to learn the typical usage of bandwidth per workstation. In cases of suddenly-increased activity, the system may allocate additional network resources for the demanding node, at the expanse of less demanding network nodes at that point in time. In cases of virus outbursts, flood attempts and denial-of-service attacks against unique resources within the network, the system intrudes and decreases the bandwidth being consumed by the specific network nodes.

Figure 3 is a block diagram illustrating the principle hardware modules of the system. Information packets 300 from the network flow into the system 200, defragmented at the fragment assembly component 310 and are parsed by the packet parsing 320. Data is then analyzed by the expert system's 330 components: the filter 331, the IP anti-spoofing component 332 and the string matching accelerator 333. The fuzzy logic engine 340 extrapolates the nature of the current data by relying on the system's statistical accumulated data. The system also includes a load balancing 350

and a network performance accelerator 360 components. Analysis results are presented on the system's interface 370. Data packets are then returned to the network 380.

Since the system's eavesdropping detection at layer-2 depends on keeping track of MAC-IP pair changes within the network traffic, a Dynamic Host Configuration Protocol (DHCP) analyzer serves as an integral unit within the eavesdropping detection module. At its initial operation, the system learns the address of the legitimate DHCP server within the network. This prevents DHCP spoofing attempts by confusing the network nodes and the system. As new DHCP requests are made by clients, and new IP addresses are issued by the DHCP server to arbitrary MAC addresses, Prometheus seamlessly updates its MAC-IP tables in order to maintain the correct links between NICS and issued IP addresses.

The system further includes a graphic user interface providing the network manager with diagrammatic representations of network traffic. This tool facilitates tracking abnormal communication signals, which may be identified by special patterns.

As the intrusion detection and vulnerability assessment fields become complementary to each other, a need for correlation arises in enterprise environments. Both IDS and VA systems depend on continuously updated databases for detecting new types of vulnerabilities and intrusions. The proactive knowledge of potential security breaches within the network is gained using vulnerability detection scanners. Incorporating this information into the enterprise intrusion detection system leverages the awareness to specific immediate dangers due to unpatched and/or misconfigured systems. By prioritizing actual vulnerabilities found within the internal network at the top of the intrusion detection database, based on prevalence of certain vulnerabilities, target IP addresses and monitored traffic, the system's intrusion detection technology is able to focus on the more probable dangers. Once correlation has been made between occurrence and direction of traffic, and vulnerability assessment results (possibly by 3rd

party products), percentage of false positive and false negative detections may be reduced significantly.

All applications and features described above are integrated within a standard PCI chip card which is located in a standard PC machine, such as Sun Blades, Intel Motherboards, Motorola PMC's and the like. Such implementation provides an efficient high security service quality.

What is claimed is:

1. A PCI chip card for network intrusion detection and prevention including management of network security and access control, wherein the card activity is transparent to network communication, said card comprised of:
   - monitoring module for tracking and recording data traffic on all communication layers (layer 2) wherein the data includes port switches, MAC addresses and IP Addresses;
   - learning module for recognizing anomalous traffic data within standard network signals;
   - analyzing module for identifying suspicious activity on the local network wherein the analysis is based on fuzzy logic rules which are applied on monitored data wherein recognized patterns of anomalous traffic data are used;
   - security module for alerting or activating prevention activities upon detection of suspicious activity.
2. The card of claim 1 further comprising a comparison module for checking new transmission data against authorization table of known correlation of IP addresses, port switches and MAC addresses.
3. The card of claim 1 further comprising eavesdropping prevention module for identifying Address Resolution Protocol (ARP) spoofing based on statistical analysis and layer-2 network state monitoring.
4. The card of claim 3 wherein the eavesdropping prevention module include a Dynamic Host Configuration Protocol (DHCP) analyzer.
5. The card of claim 1 wherein the prevention activities include interception of session at application level.

6. The card of claim 1 wherein the prevention activities include denying access to a specific switch block for controllable time interval or completely blocking access through a given switch port.

7. The card of claim 1 further comprising load balancing module based on analyzed traffic data.

8. The card of claim 1 further comprising a user interface module for providing graphic representations of network traffic wherein abnormal patterns of suspicious communication data are identified.

9. The card of claim 1 further comprising an assessment module for interfacing vulnerability assessment tool and improving the monitoring and analysis of network traffic data.

10. The card of claim 1 further comprising a defragmentation module for checking the data packets at their original form.

11. The card of claim 1 further comprising filtering model for checking packets headers enabling to filter data packets before reaching any software modules, wherein the filtering is based on source/destination MAC and IP addresses, network ports, switch ports or protocol type data stored in the card memory.

12. The card of claim 1 further comprising a traffic normalization module based on bargain-point equilibrium formulas, for achieving a state of relatively fair allocation of bandwidth among network nodes, wherein allocation is based on statistical history data of typical usage of bandwidth per workstation and online behavior of the consumed bandwidth per specific network nodes.

Figure 1

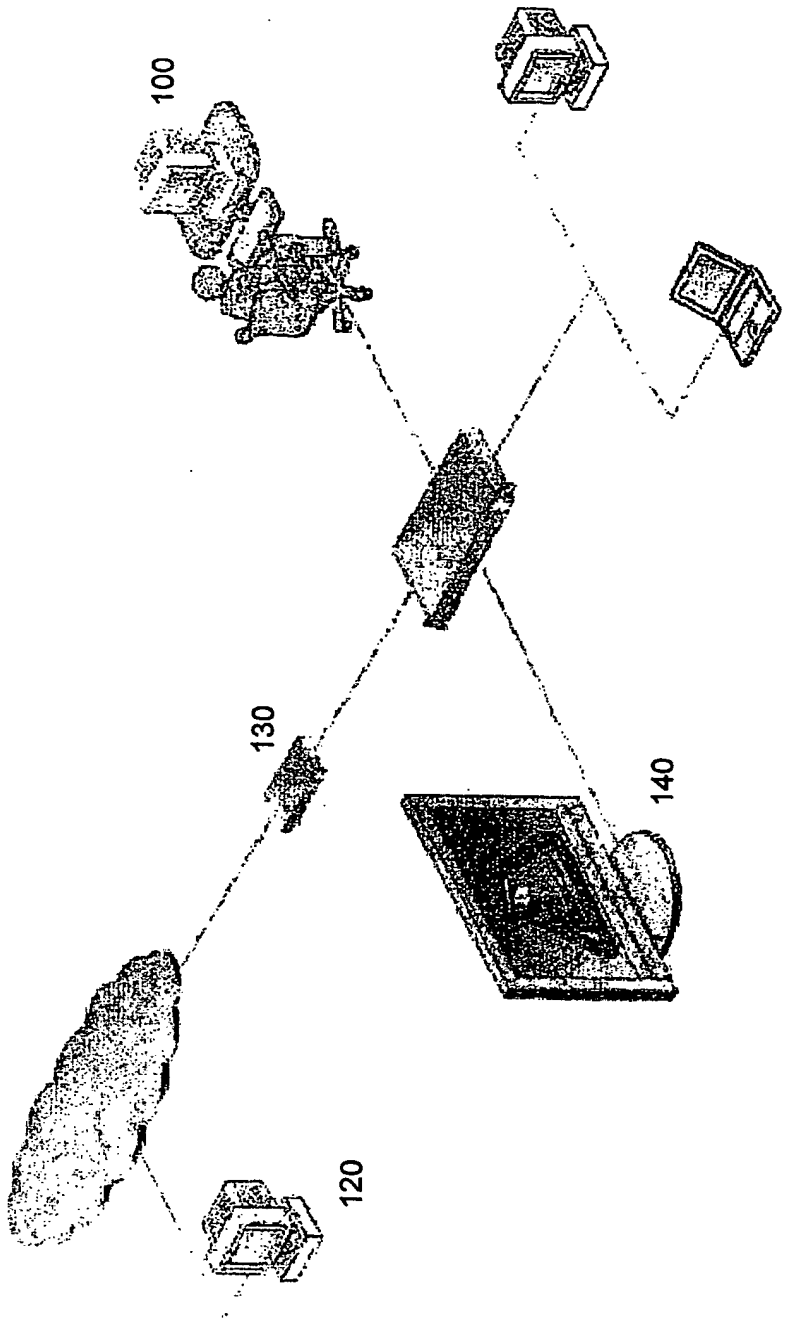


Figure 2

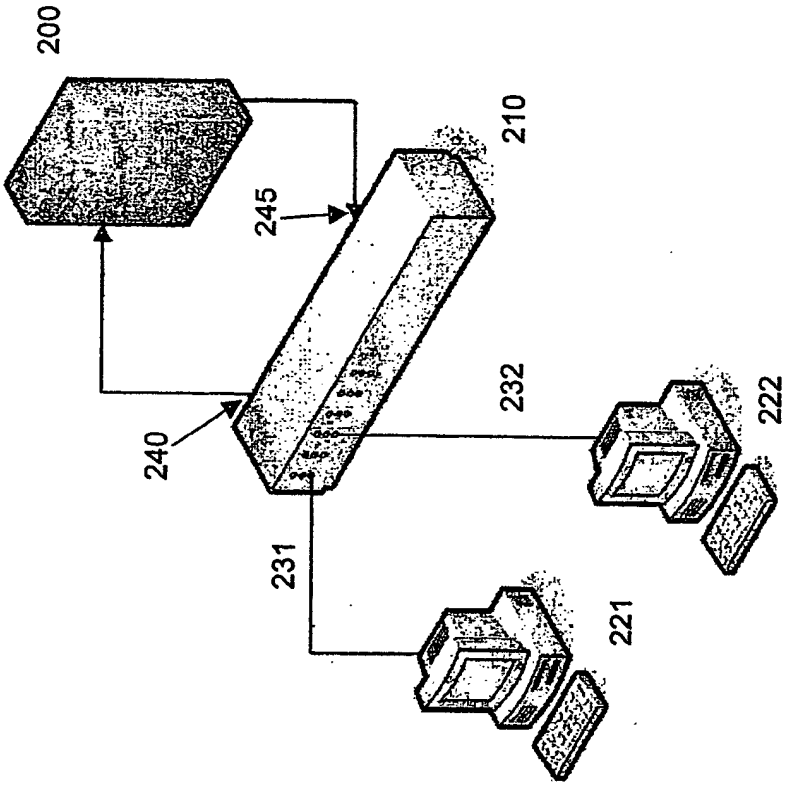
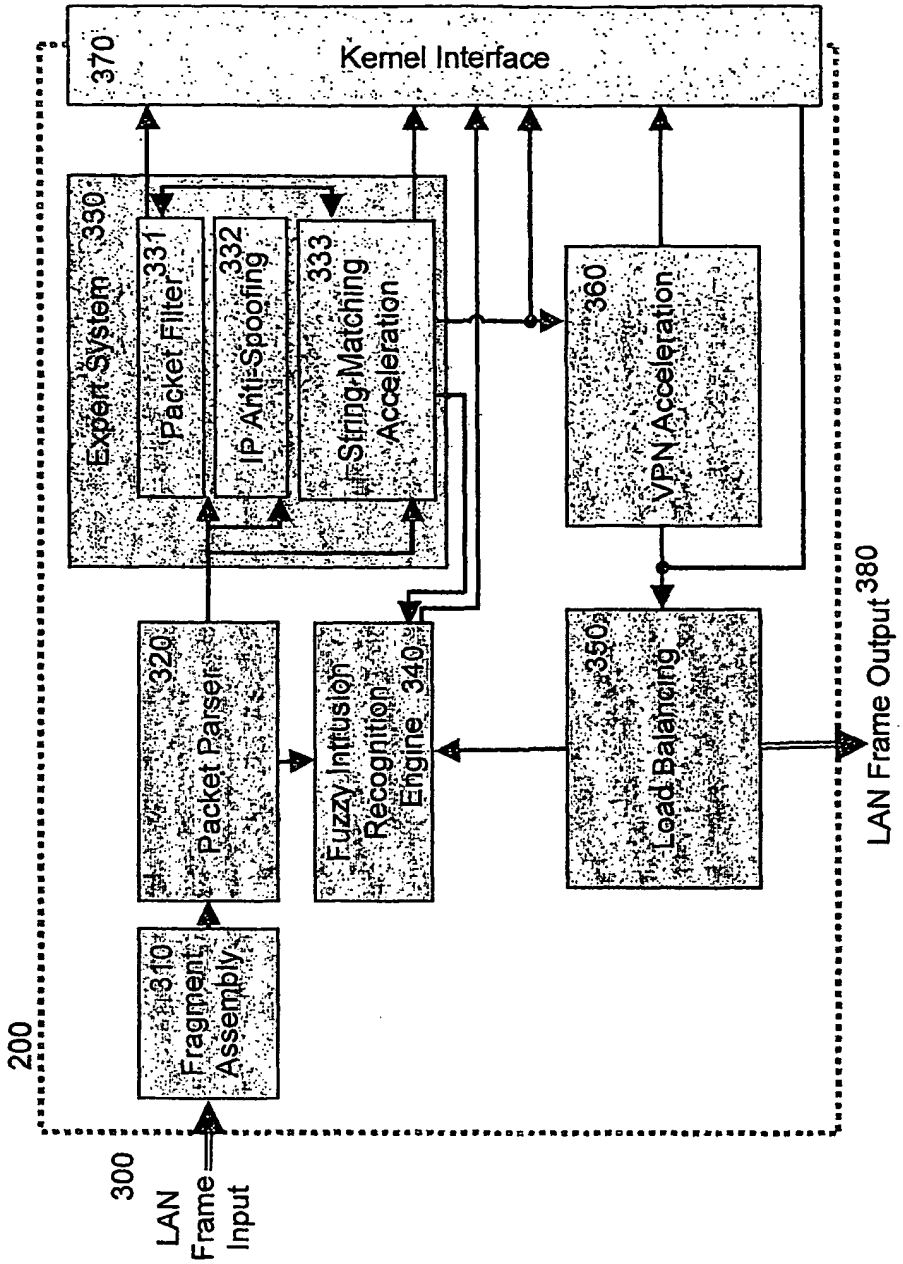


Figure 3


370
Kernel Interface
330
Expert System
331
Packet Filter
332
IP Anti-Spoofing
333
String Matching Acceleration
360
VPN Acceleration
320
Packet Parser
340
Fuzzy Intrusion Recognition Engine
350
Load Balancing
380
LAN Frame Output
310
Fragment Assembly
200
300
LAN Frame Input

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 March 2005 (24.03.2005)

PCT

(10) International Publication Number
WO 2005/026872 A3

(51) International Patent Classification[7]: G06F 11/30, 12/14, H04L 9/00, 9/32

(21) International Application Number: PCT/IL2004/000849

(22) International Filing Date: 14 September 2004 (14.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/502,940 16 September 2003 (16.09.2003) US

(71) Applicant *(for all designated States except US)*: TERASSIC-5 INFOSEC LTD [IL/IL]; 25 Yam Hamelah st., 55900 Ganey -Tikva (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: RAVIV, Raz [IL/IL]; 25 Yam Hamelah st., 55900 Ganey -Tikva (IL).

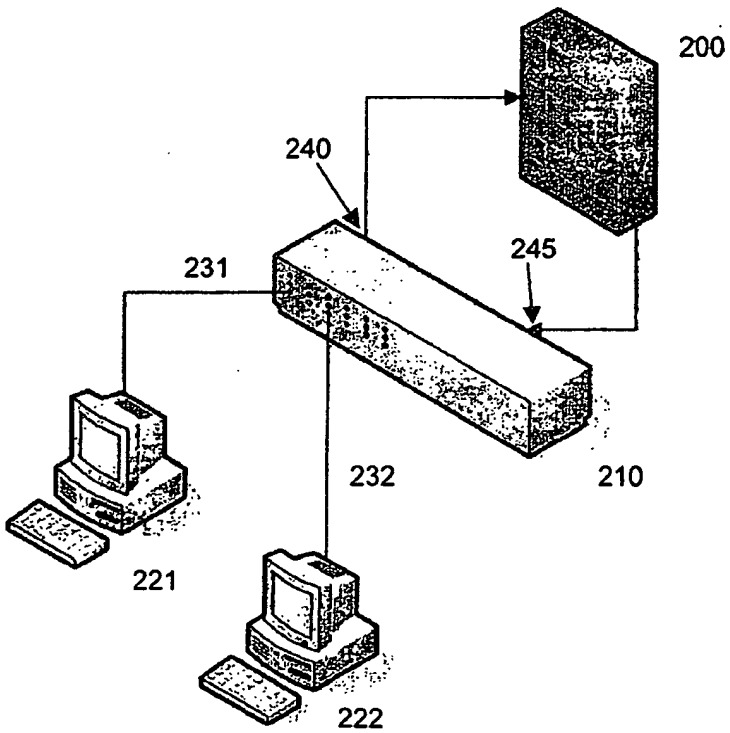
(74) Agent: APPELFELD ZER LAW OFFICE; 29 Lilinblum, 65133 Tel-aviv (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: INTERNAL LAN PERIMETER SECURITY APPLIANCE COMPOSED OF A PCI CARD AND COMPLEMENTARY SOFTWARE



(57) Abstract: A system for providing LAN security which operates on communication Layers 2 to 7 is disclosed. The system is comprised of a PCI card which performs the monitoring of the communication on the LAN, statistical analysis of data traffic and implements fuzzy logic and protocol flow inspection for identifying any abnormal and suspicious communication activity. It is composed of a hardware network interface, whose presence on the network is invisible to the network users, and of an additional interface issuing session interception signals. Using discriminate functions classing, the system can learn to recognize and differentiate anomalous traffic within standard network signals. The system is equipped for rapid recognition of known and unknown malicious activities within routine network traffic. Coupled with known protocol flow comparison, the system detects masquerading, eavesdropping, scanning, denial-of-service attacks and "hacking" attempts. The system also performs network communication flow optimization and hardware performance enhancement.

WO 2005/026872 A3

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
19 May 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL04/00849

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/30, 12/14; H04L 9/00, 9/32
US CL : 713/200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,304,973 B1 (Williams) 16 Oct. 2001 (16.10.2001), column 6-column 17	1-2, 5-6, 10-11
---		---
Y		3-4, 7-9, 12
Y	US 6,292,838 B1 (Nelson) 18 Sep. 2001 (18.09.2001), column 10, lines 4-28	3
Y	US 2003/0009540 A1(Benefield et al.) 09 Jan. 2003 (09.01.2003), paragraphs 196, 280, and Figure 9A	4, 8
Y	US 2002/0107953 A1 (Ontiveros et al.) 8 Aug. 2002 (8.08.2002), paragraphs 10, 23-33	7, 9, 12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
17 March 2005 (17.03.2005)

Date of mailing of the international search report
15 APR 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
for Michelle L. Ecoe
Albert Decady

Telephone No. (571) 272-3819

Form PCT/ISA/210 (second sheet) (January 2004)